

1 GERALD S. OHN (SBN 217382)  
gerald@ohnlaw.com  
2 **LAW OFFICES OF GERALD S. OHN, APC**  
25129 The Old Road, Suite 207  
3 Stevenson Ranch, CA 91381  
4 Telephone: (661) 475-5220  
5 Facsimile: (310) 694-3049  
6 Attorney for Plaintiff

7  
8 UNITED STATES DISTRICT COURT  
9 CENTRAL DISTRICT OF CALIFORNIA  
10 WESTERN DIVISION  
11

12 GRACE CHO, on behalf of herself and  
13 all others similarly situated,

14 Plaintiff,

15 v.

16 EQUIFAX, INC.; and DOES 1 through  
17 10, inclusive,

18 Defendants.  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

Case No.

**CLASS ACTION COMPLAINT**

**DEMAND FOR JURY TRIAL**

1 Plaintiff Grace Cho (“Plaintiff”), individually and on behalf of the classes  
2 defined below, brings this Class Action Complaint (“Complaint”) against defendant  
3 Equifax, Inc. (“Equifax”), based upon personal knowledge with respect to herself  
4 and on information and belief derived from, among other things, investigation of  
5 counsel and review of public documents as to all other matters, and allege as  
6 follows:

## 7 INTRODUCTION

8 1. On September 7, 2017, Equifax announced a nationwide data breach  
9 affecting an estimated 143 million consumers (the “Data Breach”). According to  
10 Equifax’s press release and other public statements, unauthorized parties accessed  
11 consumers’ sensitive, personal information maintained by Equifax by exploiting a  
12 website application vulnerability. Equifax claims that based on its investigation, the  
13 unauthorized access occurred from mid-May through July 2017. The information  
14 included names, addresses, Social Security numbers, dates of birth, and, in some  
15 instances, driver’s license numbers. Equifax also admitted that credit card numbers  
16 for approximately 209,000 consumers, and certain dispute documents with personal  
17 identifying information (“PII”) for approximately 182,000 consumers were  
18 accessed.

19 2. The Data Breach occurred because Equifax failed to implement adequate  
20 security measures to safeguard Plaintiff’s and other consumers’ PII and willfully  
21 ignored known weaknesses in its data security, including prior hacks into its  
22 information systems. Unauthorized parties routinely attempt to gain access to and  
23 steal personal information from networks and information systems—especially  
24 from entities such as Equifax, which are known to possess a large number of  
25 individuals’ valuable personal and financial information.

26 3. Armed with the personal information obtained in the Data Breach,  
27 identity thieves can commit a variety of crimes that harm victims of the Data  
28 Breach. For instance, they can take out loans, mortgage property, and open

1 financial accounts and credit cards in a victim's name; use a victim's information to  
2 obtain government benefits or file fraudulent returns to obtain a tax refund; obtain a  
3 driver's license or identification card in a victim's name; gain employment in a  
4 victim's name; obtain medical services in a victim's name; or give false  
5 information to police during an arrest. Hackers also routinely sell individuals' PII to  
6 other criminals who intend to misuse the information.

7 4. As a result of Equifax's willful failure to prevent the Data Breach,  
8 Plaintiff and class members have been exposed to fraud, identity theft, and financial  
9 harm, as detailed below, and to a heightened, imminent risk of such harm in the  
10 future. Plaintiff and class members have to monitor their financial accounts and  
11 credit histories more closely and frequently to guard against identity theft. Class  
12 members also have incurred, and will continue to incur, additional out-of-pocket  
13 costs for obtaining credit reports, credit freezes, credit monitoring services, and  
14 other protective measures in order to detect, protect, and repair the Data Breach's  
15 impact on their PII for the remainder of their lives. Plaintiff has already spent time  
16 addressing the Data Breach. Plaintiff anticipates spending considerable time and  
17 money for the rest of his life in order to detect and respond to the impact of the  
18 Data Breach.

19 5. There is a strong likelihood that class members already have or will  
20 become victims of identity fraud given the breadth of their PII that is now publicly  
21 available. Javelin Strategy & Research reported in its 2014 Identity Fraud Study  
22 that "[d]ata breaches are the greatest risk factor for identity fraud." In fact, "[i]n  
23 2013, one in three consumers who received notification of a data breach became a  
24 victim of fraud." Javelin also found increased instances of fraud other than credit  
25 card fraud, including "compromised lines of credit, internet accounts (e.g., eBay,  
26 Amazon) and email payment accounts such as PayPal."  
27  
28



1 credit card was then used to make unauthorized purchases in a total amount of over  
2 \$14,000. After Plaintiff received notice of the Data Breach and was informed that  
3 she was impacted by the Data Breach, Plaintiff spent at least several hours  
4 addressing the impact and potential future impact of the Data Breach. Plaintiff has  
5 also spent time and effort monitoring her financial accounts, and anticipates  
6 spending more time and effort monitoring her financial accounts in the future as a  
7 result of the Data Breach.

## 8 **Defendants**

9 11. Equifax is a Delaware corporation with its principal place of business  
10 located at 1550 Peachtree Street NE, Atlanta, Georgia 30309.

11 12. The true names and/or capacities, whether individual, corporate,  
12 associate or otherwise, of defendants DOES 1 through 10 inclusive, and each of  
13 them, are unknown. Plaintiff therefore sues these defendants by fictitious names.  
14 Plaintiff is informed and believes, and upon such information and belief hereby  
15 alleges, that each of the defendants and fictitiously named herein as a DOE is  
16 legally responsible, negligently or in some other manner, for the events and  
17 happenings hereinafter referred to and proximately caused the damages to Plaintiff  
18 and class members as hereinafter alleged. Plaintiff will seek leave of court to  
19 amend this Complaint to insert the true names and/or capacities of such fictitiously  
20 named defendants when the same have been ascertained.

21 13. At all times herein mentioned, defendants, and each of them, were an  
22 agent or joint venturer of each of the other defendants, and in doing the acts alleged  
23 herein, were acting with the course and scope of such agency. Each defendant had  
24 actual and/or constructive knowledge of the acts of each of the other defendants,  
25 and ratified, approved, joined in, acquiesced and/or authorized the wrongful acts of  
26 each co-defendant, and/or retained the benefits of said wrongful acts.

27 14. Defendants, and each of them, aided and abetted, encouraged and  
28 rendered substantial assistance to the other defendants in breaching their obligations

1 to Plaintiff and the members of the proposed classes, as alleged herein. In taking  
2 action, as particularized herein, to aid and abet and substantially assist the  
3 commissions of these wrongful acts and other wrongdoings complained of, each of  
4 the defendants acted with an awareness of his/her/its primary wrongdoing and  
5 realized that his/her/its conduct would substantially assist the accomplishment of  
6 the wrongful conduct, wrongful goals, and wrongdoing.

7 15. Equifax is one of the major credit reporting bureaus in the United States.  
8 As a credit bureau service, Equifax is engaged in a number of credit-related  
9 services for individuals, businesses, and compliance with government regulations.  
10 Specifically, Equifax provides business services to the automotive, communications,  
11 utilities and digital media, education, financial services, healthcare, insurance,  
12 mortgage, restaurant, retail and wholesale trade, staffing, and transportation and  
13 distribution industries. Equifax markets and sells many products to consumers and  
14 businesses, including Consumer Reports, which provides “access to current  
15 personally identifiable information for over 210 million consumers.” Equifax’s  
16 Consumer Reports also includes “tradelines on over 1.8 billion trades updated  
17 monthly” and “600 million unique, annual inquiries.” Equifax’s Consumer Reports  
18 provides “access to the consumer’s name, current address, address, previous former  
19 addresses, birth date, former names and Social Security number.” Equifax’s  
20 Consumer Reports is a product designed to “increase revenue”.

## 21 **STATEMENT OF FACTS**

### 22 **The Data Breach Compromised the PII of 143 Million Consumers**

23 16. On September 7, 2017, Equifax announced that its systems had been  
24 breached and that the Data Breach affected approximately 143 million consumers.  
25 According to Equifax’s website regarding the Data Breach, unauthorized users  
26 acquired the PII of approximately 143 million consumers from certain files  
27 maintained and stored by Equifax. The PII included names, addresses, Social  
28 Security numbers, dates of birth, and, in some instances, driver’s license numbers,

1 and other personal information.

2 17. On its website, Equifax admits learning of the Data Breach on July 29,  
3 2017, but only began notifying consumers through a press release and  
4 genericwebsite at <https://www.equifaxsecurity2017.com> on September 7, 2017,  
5 almost four months after the Data Breach began.

6 18. Instead of immediately notifying consumers when it discovered the  
7 Data Breach, Equifax executives sold at least \$1.8 million worth of shares before  
8 the public disclosure of the breach. It has been reported that its Chief Financial  
9 Officer John Gamble sold shares worth \$946,374, its president of U.S. information  
10 solutions, Joseph Loughran, exercised options to dispose of stock worth \$584,099,  
11 and its president of workforce solutions, Rodolfo Ploder, sold \$250,458 of stock on  
12 August 2, 2017.

13 19. In response to the questions of “Why am I learning about this incident  
14 through the media?” and “Why didn’t Equifax notify me directly?”, Equifax states  
15 that it “issued a national press release in order to notify U.S. consumers of this  
16 incident and has established a website, [www.equifaxsecurity2017.com](http://www.equifaxsecurity2017.com), where U.S.  
17 consumers can receive further information.”

18 20. Despite the fact that Equifax has the names and addresses for the 143  
19 million U.S. Data Breach victims, Equifax has not provided direct mail notices to  
20 them; rather, Equifax states that it will only provide direct mail notice to the  
21 209,000 consumers whose credit card numbers and 182,000 consumers whose  
22 dispute documents with PII were impacted.

23 21. On its website, Equifax admits the unauthorized disclosure of consumer  
24 data.

25 22. On its Data Breach website, Equifax invites individuals to determine if  
26 their personal information may have been impacted by the Data Breach by  
27 providing their last name and the last six digits of their Social Security number. If  
28 an individual is determined to have been affected, Equifax provides them with a

1 date to return to the website to enroll in Equifax's TrustedID Premier credit  
2 monitoring service. If an individual is determined to have not been affected,  
3 Equifax provides them with this information, but then still provides them with a  
4 link to enroll in (and pay for) Equifax's TrustedID Premier credit monitoring  
5 service.

6 **Equifax Promised to Protect its Customers' PII, but Maintained Inadequate**  
7 **Data Security**

8 23. Equifax is one of the major credit reporting bureaus in the United  
9 States. As a credit bureau service, Equifax is engaged in a number of credit-related  
10 services for individuals, businesses, and compliance with government regulations.  
11 Specifically, Equifax provides business services to the automotive, communications,  
12 utilities and digital media, education, financial services, healthcare, insurance,  
13 mortgage, restaurant, retail and wholesale trade, staffing, and transportation and  
14 distribution industries. Equifax markets and sells many products to consumers and  
15 businesses, including Consumer Reports, which provides "access to current  
16 personally identifiable information for over 210 million consumers." Equifax's  
17 Consumer Reports also includes "tradelines on over 1.8 billion trades updated  
18 monthly" and "600 million unique, annual inquiries." Equifax's Consumer Reports  
19 provides "access to the consumer's name, current address, address, previous former  
20 addresses, birth date, former names and Social Security number."

21 24. Prior to the Data Breach, Equifax promised its customers and everyone  
22 else whose PII it collects that it would reasonably protect their PII. Equifax's  
23 privacy policy stated, in relevant part: "We have built our reputation on our  
24 commitment to deliver reliable information to our customers (both businesses  
25 and consumers) and to protect the privacy and confidentiality of personal  
26 information about consumers. We also protect the sensitive information we have  
27 about businesses. Safeguarding the privacy and security of information, both  
28 online and offline, is a top priority for Equifax."



1 25. Equifax's policy further stated:

2 We are committed to protecting the security of your information through  
3 procedures and technology designed for this purpose by taking these steps:

- 4 • We limit access to your personal information to employees having a  
5 reasonable need to access this information to provide products and  
6 services to you. Employees who misuse information are subject to  
7 disciplinary action, including termination.
- 8 • We have reasonable physical, technical and procedural safeguards to help  
9 protect your personal information.
- 10 • In areas that contain your personal information, we use secure socket  
11 layer (SSL) encryption to help protect this information while it is in  
12 transit between our servers and your computer.

13 26. Plaintiff and Class members disclosed their PII to Equifax in connection  
14 with consumer transactions and Equifax compiled, maintained, furnished, and made  
15 available Plaintiff's and Class members' PII. Equifax was allowed to perform such  
16 services involving sensitive information only if it adhered to the requirements of  
17 laws meant to protect the privacy of such information, such as the FCRA and the  
18 Gramm-Leach-Bliley Act ("GLBA"). Equifax's maintenance, use, and furnishing  
19 of such PII is and was intended to affect Plaintiff and other Class members, and the  
20 harm caused by disclosure of that PII in the Data Breach was entirely foreseeable to  
21 Equifax.

22 **Equifax Experienced Prior Data Breaches, but Nevertheless Failed to**  
23 **Implement Appropriate Security**

24 27. Although Equifax claims to be a leader in data security and its privacy  
25 policy promises to reasonably safeguard consumer data, Equifax's own data  
26 security practices were inadequate. Equifax was well aware of this fact because it  
27 had experienced multiple data breaches in recent years.

28 28. In March 2014, Equifax reported a data breach to the New Hampshire

1 Attorney General involving an IP address operator who was able to obtain Equifax  
2 consumer credit reports using sufficient personal information to bypass Equifax's  
3 identity verification process.

4 29. In May 2016, Equifax's W-2 Express website suffered a data breach  
5 where an attacker was able to access, download and post the names, addresses,  
6 social security numbers and other personal information of over 430,000 Kroger  
7 employees. The attackers were able to access the W-2 data by merely entering  
8 Equifax's portal with an employee's default PIN code, which was the last four  
9 digits of the employee's Social Security number and their four-digit birth year.<sup>16</sup>

10 30. Independent security researchers have also found that Equifax's  
11 website is vulnerable. In 2016, a security researcher found a common vulnerability  
12 known as cross-site scripting (XSS) on the main Equifax website. Such XSS bugs  
13 allow attackers to send specially-crafted links to Equifax customers and, if the  
14 target clicks through and is logged into the site, their username and password can  
15 be revealed to the hacker.

16 31. Researcher Kenneth White just recently discovered a link in the source  
17 code on the Equifax consumer sign-in page that pointed to Netscape, a web browser  
18 that was discontinued in 2008. Kevin Beaumont, a British security professional,  
19 found decade-old software in use, including IBM WebSphere, Apache Struts and  
20 Java, many of which are outdated and subject to well-known vulnerabilities.<sup>18</sup>

21 **The Data Breach has Exposed Plaintiff and Other Consumers to Fraud,**  
22 **Identity Theft, Financial Harm, and a Heightened, Imminent Risk of Such**  
23 **Harm in the Future**

24 32. Since identity thieves use the PII of other people to commit fraud or  
25 other crimes, Plaintiff and other consumers whose information was exposed in the  
26 Data Breach are subject to an increased, concrete risk of identity theft. Javelin  
27 Strategy & Research, a research-based consulting firm that specializes in fraud and  
28 security in advising its clients, reported in its 2014 Identity Fraud Study that "[d]ata

1 breaches are the greatest risk factor for identity fraud.” In fact, “[i]n 2013, one in  
2 three consumers who received notification of a data breach became a victim of  
3 fraud.” Javelin also found increased instances of fraud other than credit card fraud,  
4 including “compromised lines of credit, internet accounts (e.g., eBay, Amazon) and  
5 email payment accounts such as PayPal.”

6 33. The exposure of Plaintiff’s and class members’ Social Security  
7 numbers in particular poses serious problems. Criminals frequently use Social  
8 Security numbers to create false bank accounts, file fraudulent tax returns, and  
9 incur credit in the victim’s name. Neal O’Farrell, a security and identity theft  
10 expert for Credit Sesame calls a Social Security number “your secret sauce,” that is  
11 “as good as your DNA to hackers.” Even where data breach victims obtain a new  
12 Social Security number, the Social Security Administration warns “that a new  
13 number probably will not solve all [] problems . . . and will not guarantee [] a fresh  
14 start.” In fact, “[f]or some victims of identity theft, a new number actually creates  
15 new problems.” One of those new problems is that a new Social Security  
16 number will have a completely blank credit history, making it difficult to get credit  
17 for a few years unless it is linked to the old compromised number.

18 34. As a result of the compromising of their personal information, Plaintiff  
19 and class members will face an increased risk of experiencing the following  
20 injuries:

- 21 • money and time expended to prevent, detect, contest, and repair  
22 identity theft, fraud, and/or other unauthorized uses of personal  
23 information;
- 24 • money and time lost as a result of fraudulent access to and use of their  
25 financial accounts;
- 26 • loss of use of and access to their financial accounts and/or credit;
- 27 • impairment of their credit scores, ability to borrow, and/or ability to  
28 obtain credit;

- 1 • lowered credit scores resulting from credit inquiries following
- 2 fraudulent activities;
- 3 • costs and lost time obtaining credit reports in order to monitor their
- 4 credit records;
- 5 • money, including fees charged in some states, and time spent placing
- 6 fraud alerts and security freezes on their credit records;
- 7 • money and time expended to avail themselves of assets and/or credit
- 8 frozen or flagged due to misuse;
- 9 • costs of credit monitoring that is more robust than the services being
- 10 offered by Equifax;
- 11 • anticipated future costs from the purchase of credit monitoring and/or
- 12 identity theft protection services once the temporary services being
- 13 offered by Equifax expire;
- 14 • costs and lost time from dealing with administrative consequences of
- 15 the Data Breach, including by identifying, disputing, and seeking
- 16 reimbursement for fraudulent activity, canceling compromised financial
- 17 accounts and associated payment cards, and investigating options for
- 18 credit monitoring and identity theft protection services;
- 19 • money and time expended to ameliorate the consequences of the filing
- 20 of fraudulent tax returns;
- 21 • lost opportunity costs and loss of productivity from efforts to mitigate
- 22 and address the adverse effects of the Data Breach including, but not
- 23 limited to, efforts to research how to prevent, detect, contest, and
- 24 recover from misuse of their personal information;
- 25 • loss of the opportunity to control how their personal information is
- 26 used; and
- 27 • continuing risks to their personal information, which remains subject to
- 28 further harmful exposure and theft as long as Equifax fails to undertake

1 appropriate, legally required steps to protect the personal information in  
2 its possession.

3 35. The risks that Plaintiff and Class members bear as a result of the Data  
4 Breach cannot be mitigated by the credit monitoring Equifax has offered to affected  
5 consumers because it can only help detect, but will not prevent, the fraudulent use  
6 of Plaintiff's and class members' PII. Instead, Plaintiff and class members will need  
7 to spend time and money to protect themselves. For instance, credit reporting  
8 agencies impose fees for credit freezes in certain states. In addition, while credit  
9 reporting agencies offer consumers one free credit report per year, consumers who  
10 request more than one credit report per year from the same credit reporting agency  
11 (such as Equifax) must pay a fee for the additional report. Such fees constitute out-  
12 of-pocket costs to Plaintiff and class members.

13 36. The risks borne by affected consumers are not hypothetical: Equifax  
14 has admitted that class members' personal information was disclosed and  
15 downloaded in the Data Breach, has admitted the risks of identity theft, and has  
16 encouraged consumers to vigilantly monitor their accounts.

17 **Equifax was Required to Investigate and Provide Timely and Adequate**  
18 **Notification of the Data Breach under Federal Regulations**

19 37. The Gramm-Leach-Bliley Act ("GLBA") imposes upon "financial  
20 institutions" "an affirmative and continuing obligation to respect the privacy of its  
21 customers and to protect the security and confidentiality of those customers'  
22 nonpublic personal information." 15 U.S.C. § 6801. To satisfy this obligation,  
23 financial institutions must satisfy certain standards relating to administrative,  
24 technical, and physical safeguards: (1) to insure the security and confidentiality of  
25 customer records and information; (2) to protect against any anticipated threats or  
26 hazards to the security or integrity of such records; and (3) to protect against  
27 unauthorized access to or use of such records or information which could result in  
28 substantial harm or inconvenience to any customer. 15 U.S.C. § 6801(b).

1       38. In order to satisfy their obligations under the GLBA, financial institutions  
2 must “develop, implement, and maintain a comprehensive information security  
3 program that is [1] written in one or more readily accessible parts and [2] contains  
4 administrative, technical, and physical safeguards that are appropriate to [their] size  
5 and complexity, the nature and scope of [their] activities, and the sensitivity of any  
6 customer information at issue.” 16 C.F.R. § 314.4. “In order to develop, implement,  
7 and maintain [their] information security program, [financial institutions] shall:

8       (a) Designate an employee or employees to coordinate [their] information  
9 security program.

10       (b) Identify reasonably foreseeable internal and external risks to the security,  
11 confidentiality, and integrity of customer information that could result in  
12 the unauthorized disclosure, misuse, alteration, destruction or other  
13 compromise of such information, and assess the sufficiency of any  
14 safeguards in place to control these risks. At a minimum, such a risk  
15 assessment should include consideration of risks in each relevant area of  
16 [their] operations, including:

17       (1) Employee training and management;

18       (2) Information systems, including network and software  
19 design, as well as information processing, storage,  
20 transmission and disposal; and

21       (3) Detecting, preventing and responding to attacks, intrusions, or other  
22 systems failures.

23       (c) Design and implement information safeguards to control the risks [they]  
24 identify through risk assessment, and regularly test or otherwise monitor  
25 the effectiveness of the safeguards’ key controls, systems, and  
26 procedures.

27       (d) Oversee service providers, by:

28       (1) Taking reasonable steps to select and retain service

providers that are capable of maintaining appropriate safeguards for the customer information at issue; and

(2) Requiring [their] service providers by contract to implement and maintain such safeguards.

(e) Evaluate and adjust [their] information security program in light of the results of the testing and monitoring required by paragraph (c) of this section; any material changes to [their] operations or business arrangements; or any other circumstances that [they] know or have reason to know may have a material impact on [their] information security program.” *Id.*

39. In addition, under the Interagency Guidelines Establishing Information Security Standards, 12 C.F.R. pt. 225, App. F, financial institutions have an affirmative duty to “develop and implement a risk-based response program to address incidents of unauthorized access to customer information in customer information systems.” *See id.* “At a minimum, an institution’s response program should contain procedures for the following:

- a. Assessing the nature and scope of an incident, and identifying what customer information systems and types of customer information have been accessed or misused;
- b. Notifying its primary Federal regulator as soon as possible when the institution becomes aware of an incident involving unauthorized access to or use of sensitive customer information, as defined below;
- c. Consistent with the Agencies’ Suspicious Activity Report (“SAR”) regulations, notifying appropriate law enforcement authorities, in addition to filing a timely SAR in situations involving Federal criminal violations requiring immediate attention, such as when a reportable violation is ongoing;



- d. Taking appropriate steps to contain and control the incident to prevent further unauthorized access to or use of customer information, for example, by monitoring, freezing, or closing affected accounts, while preserving records and other evidence; and
- e. Notifying customers when warranted. *Id.*

40. Further, “[w]hen a financial institution becomes aware of an incident of unauthorized access to sensitive customer information, the institution should conduct a reasonable investigation to promptly determine the likelihood that the information has been or will be misused. If the institution determines that misuse of its information about a customer has occurred or is reasonably possible, it should notify the affected customer as soon as possible.” *See id.*

41. Credit bureaus are “financial institutions” for purposes of the GLBA, and are therefore subject to its provisions. *See TranUnion LLC v. F.T.C.*, 295 F.3d 42, 48 (D.C. Cir. 2002). Under Regulation Y promulgated by the Federal Reserve Board, Bank Holding Companies and Change in Bank Control, “credit bureau services” are “so closely related to banking or managing or controlling banks as to be a proper incident thereto.” Since Equifax is a credit bureau and performs credit bureau services, it qualifies as a financial institution for purposes of the GLBA.

42. “Nonpublic personal information,” includes PII (such as the PII compromised during the Data Breach) for purposes of the GLBA. Likewise, “sensitive customer information” includes PII for purposes of the Interagency Guidelines Establishing Information Security Standards.

43. Upon information and belief, Equifax failed to “develop, implement, and maintain a comprehensive information security program” with “administrative, technical, and physical safeguards” that were “appropriate to [its] size and complexity, the nature and scope of [its] activities, and the sensitivity of any customer information at issue.” This includes, but is not limited to, (a) Equifax’s failure to implement and maintain adequate data security practices to safeguard



1 class members' PII; (b) failing to detect the Data Breach in a timely manner; and (c)  
2 failing to disclose that its data security practices were inadequate to safeguard class  
3 members' PII.

4 44. Upon information and belief, Equifax also failed to "develop and  
5 implement a risk-based response program to address incidents of unauthorized  
6 access to customer information in customer information systems" as mandated by  
7 the GLBA. This includes, but is not limited to, Equifax's failure to notify  
8 appropriate regulatory agencies, law enforcement, and the affected individuals  
9 themselves of the Data Breach in a timely and adequate manner.

10 45. Upon information and belief, Equifax also failed to notify affected  
11 customers as soon as possible after it became aware of unauthorized access to  
12 sensitive customer information.

### 13 **CLASS ALLEGATIONS**

14 46. Plaintiff seeks certification under Federal Rule of Civil  
15 Procedure 23(b)(1), (b)(2), (b)(3), and (c)(4) and brings this action on behalf of  
16 herself and a Nationwide Class and California Subclass as follows.

17 47. Plaintiff bring her FCRA, negligence, and negligence per se claims  
18 on behalf of herself and a proposed nationwide class ("Nationwide Class"),  
19 defined as follows:

20 All natural persons and entities in the United States whose personally  
21 identifiable information was acquired by unauthorized persons in the data  
22 breach announced by Equifax in September 2017.

23 48. Plaintiff bring her state consumer protection statute and data breach  
24 notification claims on behalf of herself and a separate California Subclass.

25 49. Plaintiff also brings her negligence and negligence per se claims  
26 separately on behalf of the California Subclass, in the alternative to bringing those  
27 claims on behalf of the Nationwide Class.  
28

1       50. Except where otherwise noted, “Class Members” shall refer to members  
2 of the Nationwide Class and California Subclass, collectively.

3       51. Excluded from the Nationwide Class and California Subclass are  
4 defendants and their current employees, as well as the Court and its personnel  
5 presiding over this action.

6       52. The Nationwide and California Subclass meet the requirements of  
7 Federal Rules of Civil Procedure 23(a) and 23(b)(1), (b)(2), and (b)(3) for all of the  
8 reasons set forth below.

9       53. Numerosity: The Nationwide and California Subclass are so numerous  
10 that joinder of all members is impracticable. According to Equifax, the Nationwide  
11 Class includes approximately 143 million individuals whose PII was acquired  
12 during the Data Breach. On information and belief, Plaintiff alleges that there are  
13 millions of individuals in the California Subclass. The parties will be able to  
14 identify each member of the Nationwide Class and California Subclass after  
15 Equifax’s document production and/or related discovery.

16       54. Commonality: There are numerous questions of law and fact common  
17 to Plaintiff and the Nationwide and California Subclass including, but not limited  
18 to, the following:

- 19       • whether Equifax engaged in the wrongful conduct alleged herein;
- 20       • whether Equifax owed a duty to Plaintiff and Class Members to
- 21       adequately protect their PII;
- 22       • whether Equifax breached its duties to protect the personal information
- 23       of Plaintiff and Class Members;
- 24       • whether Equifax knew or should have known that its data security
- 25       systems and processes were vulnerable to attack;
- 26       • whether Plaintiff and Class Members suffered legally cognizable
- 27       damages as a result of Equifax’s conduct, including increased risk of
- 28       identity theft and loss of value of PII;

- whether Equifax violated the FCRA; and
- whether Plaintiff and Class Members are entitled to equitable relief including injunctive relief.

55. Typicality: Plaintiff's claims are typical of the claims of the Nationwide Class, and Plaintiff's claims are typical of the claims of the California Subclass. Plaintiff, like all proposed Class Members, had his PII compromised in the Data Breach.

56. Adequacy: Plaintiff will fairly and adequately protect the interests of the Nationwide Class and California Subclass. Plaintiff has no interests that are adverse to, or in conflict with, the Class Members. There are no claims or defenses that are unique to Plaintiff. Likewise, Plaintiff has retained counsel experienced in class action and complex litigation, including data breach litigation, that have sufficient resources to prosecute this action vigorously.

57. Predominance: The proposed action meets the requirements of Federal Rule of Civil Procedure 23(b)(3) because questions of law and fact common to the Nationwide Class and California Subclass predominate over any questions which may affect only individual Class members in any of the proposed classes, including those listed above.

58. Superiority: The proposed action also meets the requirements of Federal Rule of Civil Procedure 23(b)(3) because a class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions is superior to multiple individual actions or piecemeal litigation, avoids inconsistent decisions, presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of the Class Members.

59. Absent a class action, the majority of Class Members would find the cost of litigating their claims prohibitively high and would have no effective remedy.

60. Risks of Prosecuting Separate Actions: Plaintiff's claims also meet the requirements of Federal Rule of Civil Procedure 23(b)(1) because prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications that would establish incompatible standards for Equifax. Equifax continues to maintain the PII of the Class Members and other individuals, and varying adjudications could establish incompatible standards with respect to: Equifax's duty to protect individuals' PII; whether Equifax's ongoing conduct violates the FCRA and other claims alleged herein; and whether the injuries suffered by Class Members are legally cognizable, among others. Prosecution of separate actions by individual Class Members would also create a risk of individual adjudications that would be dispositive of the interests of other Class Members not parties to the individual adjudications, or substantially impair or impede the ability of Class Members to protect their interests.

61. Injunctive Relief: In addition, Equifax has acted and/or refused to act on grounds that apply generally to the Nationwide and California Subclass, making injunctive and/or declaratory relief appropriate with respect to the classes under Federal Rule of Civil Procedure 23(b)(2). Equifax continues to (1) maintain the PII of Class Members, (2) fail to adequately protect their PII, and (3) violate their rights under the FCRA and other claims alleged herein.

62. Certification of Particular Issues: In the alternative, the Nationwide Class and California Subclass may be maintained as class actions with respect to particular issues, in accordance with Fed. R. Civ. P. 23(c)(4).

## CLAIMS FOR RELIEF

### FIRST CLAIM FOR RELIEF

#### WILLFUL VIOLATION OF THE FAIR CREDIT REPORTING ACT

63. Plaintiff incorporates by reference all paragraphs above as if fully set forth herein.

64. As individuals, Plaintiff and Class Members are consumers entitled

1 to the protections of the FCRA. 15 U.S.C. § 1681a(c).

2 65. Under the FCRA, a “consumer reporting agency” is defined as “any  
3 person which, for monetary fees, dues, or on a cooperative nonprofit basis,  
4 regularly engages in whole or in part in the practice of assembling or evaluating  
5 consumer credit information or other information on consumers for the purpose  
6 of furnishing consumer reports to third parties . . . .” 15 U.S.C. § 1681a(f).

7 66. Equifax is a consumer reporting agency under the FCRA because for  
8 monetary fees, it regularly engages in the practice of assembling or evaluating  
9 consumer credit information or other information on consumers for the purpose  
10 of furnishing consumer reports to third parties.

11 67. As a consumer reporting agency, the FCRA requires Equifax to  
12 “maintain reasonable procedures designed to . . . limit the furnishing of consumer  
13 reports to the purposes listed under section 1681b of this title.” 15 U.S.C. §  
14 1681e(a).

15 68. Under the FCRA, a “consumer report” is defined as “any written, oral, or  
16 other communication of any information by a consumer reporting agency bearing  
17 on a consumer’s credit worthiness, credit standing, credit capacity, character,  
18 general reputation, personal characteristics, or mode of living which is used or  
19 expected to be used or collected in whole or in part for the purpose of serving as a  
20 factor in establishing the consumer’s eligibility for - - (A) credit . . . to be used  
21 primarily for personal, family, or household purposes; . . . or (C) any other purpose  
22 authorized under section 1681b of this title.” 15 U.S.C. § 1681a(d)(1).

23 69. The compromised data was a consumer report under the FCRA because it  
24 was a communication of information bearing on Class members’ credit worthiness,  
25 credit standing, credit capacity, character, general reputation, personal  
26 characteristics, or mode of living used, or expected to be used or collected in whole  
27 or in part, for the purpose of serving as a factor in establishing the Class members’  
28 eligibility for credit.

1       70. As a consumer reporting agency, Equifax may only furnish a consumer  
2 report under the limited circumstances set forth in 15 U.S.C. § 1681b, “and no  
3 other.” 15 U.S.C. § 1681b(a). None of the purposes listed under 15 U.S.C. § 1681b  
4 permit credit reporting agencies to furnish consumer reports to unauthorized or  
5 unknown entities, or computer hackers such as those who accessed the Nationwide  
6 Class members’ PII. Equifax violated § 1681b by furnishing consumer reports to  
7 unauthorized or unknown entities or computer hackers, as detailed above.

8       71. Equifax furnished the Nationwide Class members’ consumer reports by  
9 disclosing their consumer reports to unauthorized entities and computer hackers;  
10 allowing unauthorized entities and computer hackers to access their consumer  
11 reports; knowingly and/or recklessly failing to take security measures that would  
12 prevent unauthorized entities or computer hackers from accessing their consumer  
13 reports; and/or failing to take reasonable security measures that would prevent  
14 unauthorized entities or computer hackers from accessing their consumer reports.

15       72. The Federal Trade Commission (“FTC”) has pursued enforcement  
16 actions against consumer reporting agencies under the FCRA for failing “take  
17 adequate measures to fulfill their obligations to protect information contained in  
18 consumer reports, as required by the” FCRA, in connection with data breaches.

19       73. Equifax willfully violated § 1681b and § 1681e(a) by providing  
20 impermissible access to consumer reports and by failing to maintain reasonable  
21 procedures designed to limit the furnishing of consumer reports to the purposes  
22 outlined under section 1681b of the FCRA. The willful nature of Equifax’s  
23 violations is supported by, among other things, former employees’ admissions  
24 that Equifax’s data security practices have deteriorated in recent years, and  
25 Equifax’s numerous other data breaches in the past. Further, Equifax touts itself as  
26 an industry leader in breach prevention; thus, Equifax was well aware of the  
27 importance of the measures organizations should take to prevent data breaches, and  
28 willingly failed to take them.

74. Equifax also acted willfully because it knew or should have known about its legal obligations regarding data security and data breaches under the FCRA. These obligations are well established in the plain language of the FCRA and in the promulgations of the Federal Trade Commission. *See, e.g.*, 55 Fed. Reg. 18804 (May 4, 1990), 1990 Commentary On The Fair Credit Reporting Act. 16 C.F.R. Part 600, Appendix To Part 600, Sec. 607 2E. Equifax obtained or had available these and other substantial written materials that apprised them of their duties under the FCRA. Any reasonable consumer reporting agency knows or should know about these requirements. Despite knowing of these legal obligations, Equifax acted consciously in breaching known duties regarding data security and data breaches and depriving Plaintiff and other members of the classes of their rights under the FCRA.

75. Equifax's willful and/or reckless conduct provided a means for unauthorized intruders to obtain and misuse Plaintiff's and Nationwide Class members' personal information for no permissible purposes under the FCRA.

76. Plaintiff and the Nationwide Class Members have been damaged by Equifax's willful failure to comply with the FCRA. Therefore, Plaintiff and each of the Nationwide Class members are entitled to recover "any actual damages sustained by the consumer . . . or damages of not less than \$100 and not more than \$1,000." 15 U.S.C. § 1681n(a)(1)(A).

77. Plaintiff and the Nationwide Class members are also entitled to punitive damages, costs of the action, and reasonable attorneys' fees. 15 U.S.C. § 1681n(a)(2), (3).

## **SECOND CLAIM FOR RELIEF**

### **NEGLIGENT VIOLATION OF THE FAIR CREDIT REPORTING ACT**

78. Plaintiff incorporates by reference all paragraphs above as if fully set forth here.



1       79. Equifax was negligent in failing to maintain reasonable procedures  
2 designed to limit the furnishing of consumer reports to the purposes outlined under  
3 section 1681b of the FCRA. Equifax's negligent failure to maintain reasonable  
4 procedures is supported by, among other things, former employees' admissions that  
5 Equifax's data security practices have deteriorated in recent years, and Equifax's  
6 numerous other data breaches in the past. Further, as an enterprise claiming to be  
7 an industry leader in data breach prevention, Equifax was well aware of the  
8 importance of the measures organizations should take to prevent data breaches, yet  
9 failed to take them.

10       80. Equifax's negligent conduct provided a means for unauthorized  
11 intruders to obtain Plaintiff's and the Nationwide Class members' PII and consumer  
12 reports for no permissible purposes under the FCRA.

13       81. Plaintiff and the Nationwide Class members have been damaged by  
14 Equifax's negligent failure to comply with the FCRA. Therefore, Plaintiff and each  
15 of the Nationwide Class members are entitled to recover "any actual damages  
16 sustained by the consumer." 15 U.S.C. § 1681o(a)(1).

17       82. Plaintiff and the Nationwide Class members are also entitled to recover  
18 their costs of the action, as well as reasonable attorneys' fees. 15 U.S.C. §  
19 1681o(a)(2).

### 20                               **THIRD CLAIM FOR RELIEF**

#### 21                                       **NEGLIGENCE**

22       83. Plaintiff incorporates by reference all paragraphs above as if fully set  
23 forth here.

24       84. Equifax owed a duty to Plaintiff and Class Members, arising from the  
25 sensitivity of the information and the foreseeability of its data safety shortcomings  
26 resulting in an intrusion, to exercise reasonable care in safeguarding their sensitive  
27  
28



1 personal information. This duty included, among other things, designing  
2 maintaining, monitoring, and testing Equifax's security systems, protocols,  
3 and practices to ensure that Class Members' information adequately secured from  
4 unauthorized access.

5 85. Equifax's privacy policy acknowledged Equifax's duty to adequately  
6 protect Class Members' PII.

7 86. Equifax owed a duty to Class Members to implement current and  
8 available technology that would prevent foreseeable data breaches, such as this one.

9 87. Equifax owed a duty to Class Members to implement intrusion  
10 detection processes that would detect a data breach in a timely manner.

11 88. Equifax also had a duty to delete any PII that was no longer needed to  
12 serve client needs.

13 89. Equifax owed a duty to disclose the material fact that its data security  
14 practices were inadequate to safeguard Class Members' PII.

15 90. Equifax also had independent duties under Plaintiff's and Class  
16 Members' state laws that required Equifax to reasonably safeguard Plaintiff's and  
17 Class Members' PII and promptly notify them about the Data Breach.

18 91. Equifax had a special relationship with Plaintiff and Class Members  
19 from being entrusted with their PII, which provided an independent duty of care.  
20 Plaintiff's and other Class Members' willingness to entrust Equifax with their PII  
21 was predicated on the understanding that Equifax would take adequate security  
22 precautions. Moreover, Equifax had the ability to protect its systems and the PII it  
23 stored on them from attack.

24 92. Equifax's role to utilize and purportedly safeguard Plaintiff's and Class  
25 Members' PII presents unique circumstances requiring a reallocation of risk.

26 93. Equifax breached its duties by, among other things: (a) failing to  
27 implement and maintain adequate data security practices to safeguard Class  
28 Members' PII; (b) failing to detect the Data Breach in a timely manner; (c) failing

1 to disclose that Equifax's data security practices were inadequate to safeguard  
2 Class Members' PII; and (d) failing to provide adequate and timely notice of the  
3 Data Breach.

4 94. But for Equifax's breach of its duties, Class Members' PII would not  
5 have been accessed by unauthorized individuals.

6 95. Plaintiff and Class Members were foreseeable victims of Equifax's  
7 inadequate data security practices. Equifax knew or should have known that a  
8 breach of its data security systems would cause damages to Class Members.

9 96. Equifax's negligent conduct provided a means for unauthorized intruders  
10 to obtain Plaintiff's and the Nationwide Class Members' PII and consumer reports  
11 for no permissible purposes under the FCRA.

12 97. As a result of Equifax's willful failure to prevent the Data Breach,  
13 Plaintiff and Class Members suffered injury which includes, but is not limited to,  
14 exposure to a heightened, imminent risk of fraud, identity theft, and financial harm.  
15 Plaintiff and Class Members must monitor their financial accounts and credit  
16 histories more closely and frequently to guard against identity theft. Class Members  
17 also have incurred, and will continue to incur on an indefinite basis, out-of-pocket  
18 costs for obtaining credit reports, credit freezes, credit monitoring services, and  
19 other protective measures to deter or detect identity theft. The unauthorized  
20 acquisition of Plaintiff's and Class Members' PII has also diminished the value of  
21 the PII.

22 98. The damages to Plaintiff and the Class Members were a proximate,  
23 reasonably foreseeable result of Equifax's breaches of its duties.

24 99. Therefore, Plaintiff and Class members are entitled to damages in an  
25 amount to be proven at trial.

**FOURTH CLAIM FOR RELIEF**  
**NEGLIGENCE PER SE**

100. Plaintiff incorporates by reference all paragraphs above as if fully set forth here.

101. Under the FCRA, 15 U.S.C. §§ 1681e, Equifax is required to “maintain reasonable procedures designed to . . . limit the furnishing of consumer reports to the purposes listed under section 1681b of this title.” 15 U.S.C. § 1681e(a).

102. Equifax failed to maintain reasonable procedures designed to limit the furnishing of consumer reports to the purposes outlined under section 1681b of the FCRA.

103. Plaintiff and Class Members were foreseeable victims of Equifax’s violation of the FCRA. Equifax knew or should have known that a breach of its data security systems would cause damages to Class members.

104. As alleged above, Equifax was required under the GLBA to satisfy certain standards relating to administrative, technical, and physical safeguards: (1) to insure the security and confidentiality of customer records and information; (2) to protect against any anticipated threats or hazards to the security or integrity of such records; and (3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.

105. In order to satisfy their obligations under the GLBA, Equifax was also required to “develop, implement, and maintain a comprehensive information security program that is [1] written in one or more readily accessible parts and [2] contains administrative, technical, and physical safeguards that are appropriate to [its] size and complexity, the nature and scope of [its] activities, and the sensitivity of any customer information at issue.” 16 C.F.R. § 314.4

106. In addition, under the Interagency Guidelines Establishing Information Security Standards, 12 C.F.R. pt. 225, App. F., Equifax had an affirmative duty to

1 “develop and implement a risk-based response program to address incidents of  
2 unauthorized access to customer information in customer information systems.”  
3 *See id.*

4 107. Further, when Equifax became aware of “unauthorized access to  
5 sensitive customer information,” it should have “conduct[ed] a reasonable  
6 investigation to promptly determine the likelihood that the information has been or  
7 will be misused” and “notif[ied] the affected customer[s] as soon as possible.” *See*  
8 *id.*

9 108. Equifax violated by GLBA by failing to “develop, implement, and  
10 maintain a comprehensive information security program” with “administrative,  
11 technical, and physical safeguards” that were “appropriate to [its] size and  
12 complexity, the nature and scope of [its] activities, and the sensitivity of any  
13 customer information at issue.” This includes, but is not limited to, Equifax’s (a)  
14 failure to implement and maintain adequate data security practices to safeguard  
15 Class Members’ PII; (b) failing to detect the Data Breach in a timely manner; and  
16 (c) failing to disclose that Equifax’s data security practices were inadequate to  
17 safeguard Class Members’ PII.

18 109. Equifax also violated the GLBA by failing to “develop and implement  
19 a risk-based response program to address incidents of unauthorized access to  
20 customer information in customer information systems.” This includes, but is not  
21 limited to, Equifax’s failure to notify appropriate regulatory agencies, law  
22 enforcement, and the affected individuals themselves of the Data Breach in a timely  
23 and adequate manner.

24 110. Equifax also violated by the GLBA by failing to notify affected  
25 customers as soon as possible after it became aware of unauthorized access to  
26 sensitive customer information.

27 111. Plaintiff and Class Members were foreseeable victims of Equifax’s  
28 violation of the GLBA. Equifax knew or should have known that its failure to take

1 reasonable measures to prevent a breach of its data security systems, and failure to  
2 timely and adequately notify the appropriate regulatory authorities, law  
3 enforcement, and Class Members themselves, would cause injury to Class  
4 Members.

5 112. Equifax's failure to comply with the applicable laws and regulations,  
6 including the FCRA and the GLBA, constitutes negligence per se.

7 113. But for Equifax's violation of the applicable laws and regulations,  
8 Class Members' PII would not have been accessed by unauthorized individuals.

9 114. As a result of Equifax's failure to comply with applicable laws and  
10 regulations, Plaintiff and Class Members suffered injury which includes, but is not  
11 limited to, exposure to a heightened, imminent risk of fraud, identity theft, and  
12 financial harm. Plaintiff and Class Members must monitor their financial accounts  
13 and credit histories more closely and frequently to guard against identity theft.  
14 Class Members also have incurred, and will continue to incur on an indefinite basis,  
15 out-of-pocket costs for obtaining credit reports, credit freezes, credit monitoring  
16 services, and other protective measures to deter or detect identity theft. The  
17 unauthorized acquisition of Plaintiff and Class Members' PII has also diminished  
18 the value of the PII.

19 115. The damages to Plaintiff and the Class Members were a proximate,  
20 reasonably foreseeable result of Equifax's breaches of applicable laws and  
21 regulations.

22 116. Therefore, Plaintiff and Class members are entitled to damages in an  
23 amount to be proven at trial.

#### 24 **FIFTH CLAIM FOR RELIEF**

#### 25 **VIOLATION OF THE CALIFORNIA UNFAIR COMPETITION LAW**

26 117. Plaintiff incorporates by reference all paragraphs above as if fully set  
27 forth herein.  
28

118. California Business & Professions Code § 17200 prohibits any “unlawful, unfair or fraudulent business act or practice and unfair, deceptive, untrue or misleading advertising.” For the reasons discussed above, Equifax violated (and continues to violate) California’s Unfair Competition Law, California Business & Professions Code §§ 17200, et seq., by engaging in the above-described unlawful, unfair, fraudulent, deceptive, untrue, and misleading acts and practices.

119. Equifax’s unfair and fraudulent acts and practices include, but are not limited to, the following:

- a. Equifax failed to enact adequate privacy and security measures, in California, to protect the Class Members’ PII from unauthorized disclosure, release, data breaches, and theft, in violation of industry standards and best practices, which was a direct and proximate cause of the Data Breach;
- b. Equifax failed to take proper action, in California, following known security risks and prior cybersecurity incidents, which was a direct and proximate cause of the Data Breach;
- c. Equifax knowingly and fraudulently misrepresented, in California, that they would maintain adequate data privacy and security practices and procedures to safeguard Class Members’ PII from unauthorized disclosure, release, data breaches, and theft;
- d. Equifax knowingly and fraudulently misrepresented that it did and would comply with the requirements of relevant federal and state laws pertaining to the privacy and security of Class members’ PII;
- e. Equifax knowingly omitted, suppressed, and concealed the inadequacy of its privacy and security protections for Class Members’ PII;

- 1 f. Equifax failed to maintain reasonable security, in violation of Cal.  
2 Civ. Code § 1798.81.5; and
- 3 g. Equifax failed to disclose the Data Breach to Class Members in a  
4 timely and accurate manner, in violation of the duties imposed by  
5 Cal. Civ. Code §§ 1798.82, et seq.

6 120. Equifax's acts and practices also constitute "unfair" business acts and  
7 practices, in that the harm caused by Equifax's wrongful conduct outweighs any  
8 utility of such conduct, and such conduct (i) offends public policy, (ii) is immoral,  
9 unscrupulous, unethical, oppressive, deceitful and offensive, and/or (iii) has caused  
10 and will continue to cause substantial injury to consumers such as Plaintiff and  
11 Class Members.

12 121. Equifax's acts and practices also constitute "unlawful" business acts  
13 and practices by virtue of their violation of the FCRA, 15 U.S.C. §§ 1681e (as  
14 described fully above), the GLBA, 15 U.S.C. § 6801 et seq. (as described fully  
15 above), California's fraud and deceit statutes, Cal. Civ. Code §§ 1572, 1573, 1709,  
16 1711; Cal. Bus. & Prof. Code §§ 17200, et seq., 17500, et seq., the California  
17 Customer Records' Act, Cal. Civ. Code §§ 1798.80, et seq. (as described fully  
18 below), and California common law.

19 122. There were reasonably available alternatives to further Equifax's  
20 legitimate business interests, including using best practices to protect Class  
21 Members' PII, other than Equifax's wrongful conduct described herein.

22 123. As a direct and/or proximate result of Equifax's unfair practices,  
23 Plaintiff, the Nationwide Class, and the California Subclass have suffered injury in  
24 fact in connection with the Data Breach including, but not limited to, the time and  
25 expenses related to monitoring their financial accounts for fraudulent activity, an  
26 increased, imminent risk of fraud and identity theft, and loss of value of their PII.  
27 As a result, Plaintiff and other Class Members are entitled to compensation,  
28

1 restitution, disgorgement, and/or other equitable relief. Cal. Bus. & Prof. Code  
2 §17203.

3 124. Equifax knew or should have known that its data security practices and  
4 infrastructure were inadequate to safeguard Class Members' PII, and that the risk of  
5 a data breach or theft was highly likely. Equifax's actions in engaging in the above  
6 named unfair practices and deceptive acts were negligent, knowing and willful,  
7 and/or wanton and reckless with respect to Class Members' rights.

8 125. On information and belief, Equifax's unlawful and unfair business  
9 practices, except as otherwise indicated herein, continue to this day and are  
10 ongoing.

11 126. Plaintiff and other Class Members also are entitled to injunctive relief,  
12 under California Business and Professions Code §§ 17203, 17204, to stop  
13 Equifax's wrongful acts and to require Equifax to maintain adequate security  
14 measures to protect the personal and financial information in its possession.

15 127. Under Business and Professions Code §§ 17200, et seq., Plaintiff seeks  
16 restitution of money or property that Equifax may have acquired by means of  
17 Equifax's deceptive, unlawful, and unfair business practices (to be proven at trial),  
18 restitutionary disgorgement of all profits accruing to Equifax because of its  
19 unlawful and unfair business practices (to be proven at trial), declaratory relief, and  
20 attorney's fees and costs (allowed by Cal. Civ. Code Proc. §1021.5).

## 21 **SIXTH CLAIM FOR RELIEF**

### 22 **VIOLATION OF THE CALIFORNIA CUSTOMER RECORDS ACT**

23 128. Plaintiff incorporates by reference all paragraphs above as if fully set  
24 forth herein.

25 129. "[T]o ensure that personal information about California residents is  
26 protected," Civil Code § 1798.81.5 requires any "business that owns, licenses, or  
27 maintains personal information about a California resident [to] implement and  
28



1 maintain reasonable security procedures and practices appropriate to the nature of  
2 the information, to protect the personal information from unauthorized access,  
3 destruction, use, modification, or disclosure.”

4 130. Equifax owns, maintains, and licenses personal information, within the  
5 meaning of § 1798.81.5, about Plaintiff and the California Subclass.

6 131. Equifax violated Civil Code § 1798.81.5 by failing to implement  
7 reasonable measures to protect Class Members’ PII.

8 132. As a direct and proximate result of Equifax’s violations of section  
9 1798.81.5 of the California Civil Code, the Data Breach described above occurred.

10 133. In addition, California Civil Code § 1798.82(a) provides that “[a]  
11 person or business that conducts business in California, and that owns or licenses  
12 computerized data that includes personal information, shall disclose a breach of the  
13 security of the system following discovery or notification of the breach in the  
14 security of the data to a resident of California whose unencrypted personal  
15 information was, or is reasonably believed to have been, acquired by an  
16 unauthorized person. The disclosure shall be made in the most expedient time  
17 possible and without unreasonable delay . . . .”

18 134. Section 1798.2(b) provides that “[a] person or business that maintains  
19 computerized data that includes personal information that the person or business  
20 does not own shall notify the owner or licensee of the information of the breach of  
21 the security of the data immediately following discovery, if the personal  
22 information was, or is reasonably believed to have been, acquired by an  
23 unauthorized person.”

24 135. Equifax is a business that own or license computerized data that includes  
25 personal information as defined by Cal. Civ. Code §§ 1798.80, et seq.

26 136. In the alternative, Equifax maintains computerized data that includes  
27 personal information that Equifax does not own as defined by Cal. Civ. Code §§  
28 1798.80, et seq.

137. Plaintiff and the California Subclass members' PII (including, but not limited to, names, addresses, and Social Security numbers) includes personal information covered by Cal. Civ. Code § 1798.81.5(d)(1).

138. Because Equifax reasonably believed that Plaintiff and the California Subclass members' personal information was acquired by unauthorized persons during the Data Breach, it had an obligation to disclose the Data Breach in a timely and accurate fashion under Cal. Civ. Code § 1798.82(a), or in the alternative, under Cal. Civ. Code § 1798.82(b).

139. By failing to disclose the Data Breach in a timely and accurate manner, Equifax violated Cal. Civ. Code § 1798.82.

140. As a direct and proximate result of Equifax's violations of sections 1798.81.5 and 1798.82 of the California Civil Code, Plaintiff and the California Subclass members suffered the damages described above including, but not limited to, time and expenses related to monitoring their financial accounts for fraudulent activity, an increased, imminent risk of fraud and identity theft, and loss of value of their PII.

141. Plaintiff and the California Subclass seek relief under § 1798.84 of the California Civil Code including, but not limited to, actual damages in an amount to be proven at trial, and injunctive relief.

### **PRAYER FOR RELIEF**

Plaintiff, on behalf of herself and all others similarly situated, request that the Court enter judgment against Equifax as follows:

- A. An order certifying this action as a class action under Federal Rule of Civil Procedure 23, defining the Class and Subclass requested herein, appointing the undersigned as Class Counsel, and finding that Plaintiff is a proper representative of the Class and Subclass requested herein;
- B. Injunctive relief requiring Equifax to (1) strengthen its data security systems that maintain PII to comply with the FCRA and GLBA, the

applicable state laws alleged herein (including, but not limited to, the California Customer Records Act) and best practices under industry standards; (2) engage third-party auditors and internal personnel to conduct security testing and audits on Equifax's systems on a periodic basis; (3) promptly correct any problems or issues detected by such audits and testing; and (4) routinely and continually conduct training to inform internal security personnel how to prevent, identify and contain a breach, and how to appropriately respond;

- C. An order requiring Equifax to pay all costs associated with class notice and administration of class-wide relief;
- D. An award to Plaintiff and all Class (and Subclass) members of compensatory, consequential, incidental, statutory and punitive damages, restitution, and disgorgement, in an amount to be determined at trial;
- E. An award to Plaintiff and all Class (and Subclass) members of additional credit monitoring and identity theft protection services beyond the one-year package Equifax is currently offering;
- F. An award of attorneys' fees, costs, and expenses, as provided by law or equity;
- G. An order requiring Equifax to pay pre-judgment and post-judgment
- H. Such other and further relief as the Court may allow.

### **DEMAND FOR JURY TRIAL**

Plaintiff demands a jury trial on all issues so triable.

Dated: November 26, 2017

Respectfully submitted,

LAW OFFICES OF GERALD S. OHN, APC

/S/ - Gerald S. Ohn

Gerald S. Ohn, Esq.

Attorney for Plaintiff